

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/517,410	03/02/2000	Stephen R. Hanna	SMY-219.01	5095

25181 7590 08/16/2004

FOLEY HOAG, LLP  
PATENT GROUP, WORLD TRADE CENTER WEST  
155 SEAPORT BLVD  
BOSTON, MA 02110

EXAMINER

ZIA, MOSSADEQ

ART UNIT PAPER NUMBER

2134

DATE MAILED: 08/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

09/517,410

Applicant(s)

HANNA ET AL.

Examiner

Mossadeq Zia

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 02 March 2000.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1,4-10,12,13 and 15-37 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1,4-10,12,13 and 15-37 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date: \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_

**DETAILED ACTION**

***Claim Rejections - 35 USC § 102***

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claim 31-34 is rejected under **35 U.S.C. 102(b)** as anticipated by Patent No.

5,748,735, Ganesan.

3. Regarding claim 31, Ganesan disclose a method for accessing information stored securely on a file server, the method comprising:

forwarding to said file server a request for information from a client (Ganesan, col. 11, line 20-21);

in response to said, request, receiving from said file server said information encrypted with a first encryption key (symmetric crypto-key) having an associated first decryption key (symmetric crypto-key) that is usable to decrypt said encrypted information (Ganesan, col. 6, line 17-20) and at least one access control list entry associated (Yaksha database, Ganesan, col. 9, line 19-20) with a client authorized to at least read said information (Ganesan, col. 11, line 25-26), said received at least one entry including said first decryption key encrypted with a second encryption key (file server's crypto-key) having an associated second decryption key (Ganesan, col. 10, line 20-21) that is usable to decrypt said encrypted first decryption key and that is accessible to said client (Ganesan, col. 6, line 49-52);

Art Unit: 2134

decrypting said encrypted first decryption key using said second decryption key to obtain said first decryption key (Ganesan, col. 6, line 52-54); and

decrypting said encrypted information using said first decryption key (Ganesan, col. 6, line 49-52).

4. Regarding claim 32, see reasoning to claim 5 stated below.

5. Regarding claims 33, 34, see reasoning to claim 6 stated below.

6. Claim 35-37 is rejected under **35 U.S.C. 102(b)** as anticipated by Patent No. 5,495,533, Linehan et al.

7. Regarding claim 35 Linehan discloses a computer program product including a computer readable medium, said computer readable medium having a file server computer program stored thereon said file server computer program for execution in a computer and comprising:

program code for storing on said file server information encrypted with a first encryption key (file encryption key) having a corresponding first decryption key that is usable to decrypt said encrypted information (Linehan, col. 10, line 39-41);

program code for storing on said file server an access control list, said access control list including at least one entry said at least one entry including said first decryption key encrypted with a second encryption key (control key, Linehan, col. 9, line 45-46) associated with one of a plurality of clients authorized (Linehan, col. 9, line 51-53) to at least read said information, and having access to a second decryption key associated with said second encryption key and usable to decrypt said encrypted first decryption key (Linehan, col. 9, line 55-56),

program code for transmitting to said one of said plurality of clients said encrypted

Art Unit: 2134

information and said at least one entry ((Linehan, col. 9, line 56-58).

8. Regarding claim 36 and 37, see reasoning for claim 35 above.

***Claim Rejections - 35 USC § 103***

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

10. Claims 1,4-7, 13-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patent No. 5,748,735, Ganesan in view of Patent No. 5,495,533, Linehan et al.

11. Regarding claim 1, Ganesan discloses a method of operation at a file server, the method comprising:

Storing (i) information encrypted with first encryption key (crypto-key, Ganesan, col. 10, line 30-34) and (ii) an access control list (authentication server, Ganesan, col. 8, line 60-61) usable by said file server to control access to said encrypted information, said access control list including an entry that includes an identifier for a client authorized to at least read said encrypted information, and a first decryption key (crypto-key) encrypted with a second encryption key (session key) wherein said first decryption key is usable to decrypt said encrypted information (Ganesan, col. 10, line 50-54), and

in response to request from said client, transmitting to said client said encrypted information and said entry (Ganesan, col. 10, line 48-49, col. 11, line 34-35).

But fails to show wherein said second encryption key is associated with a second decryption key that is usable to decrypt said encrypted first decryption key and that is accessible to said client.

However Linehan teaches that accessing user is permitted to access the data file; the key server sends the key (second decryption key) corresponding to the data file to the key client of the accessing user (accessible to client); and the key client of the accessing user uses the key to decrypt the encrypted data file (Linehan, col. 5, line 13-16).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Ganesan as per teaching of Linehan to provide an improved computing system having improved security in a distributed computing environment (Linehan, col. 4, line 26-28).

12. Regarding claim 4, Ganesan and Linehan discloses claim 1 above, and further disclose said transmitting comprises the transmitting to said client said access control list (ticket granting ticket from ticket granting server, Ganesan, col. 4, line 40-44, col. 9, 33-34).

13. Regarding claim 5, Ganesan and Linehan discloses claim 1 above, and further disclose said first encryption key and said first decryption key are symmetric (Ganesan, col. 10, line 43-44).

14. Regarding claim 6, Ganesan and Linehan discloses claim 1 above, and further disclose said first encryption key comprises one of a public key and a private key of a first public/private key pair and said first decryption key comprises the other of said public key and said private of said first public/private key pair (Ganesan, col. 10, line 44-47).

15. Regarding claim 7, Ganesan and Linehan discloses claim 1 above, and further disclose said identifier includes one of an unencrypted identifier (it is understood by the skilled artisan that a *file name* associated with stored data is an unencrypted identifier and

Art Unit: 2134

is an inherent feature of a file system that supports the file server, Ganesan, col. 11, line 58-60) and an encrypted identifier (encrypted message authentication check field, Linehan, col. 8, line 27-30).

16. Regarding claims 13, Ganesan discloses a method for securely storing information on a file server and distributing the stored information, said method comprising:

encrypting information at one of a plurality of clients in communication with said file server (Ganesan, col. 6, line 5-6, 25), said information being encrypted with a first encryption key (symmetric crypto-key) having an associated first decryption key (symmetric crypto-key) that is usable to decrypt said encrypted information (Ganesan, col. 6, line 17-20);

encrypting said first decryption key with a second encryption key (file server's crypto-key) for each of said plurality of clients authorized to at least read said information (Ganesan, col. 6, line 20-21), wherein each respective one of said second encryption keys has a corresponding second decryption key that is usable to decrypt said respective encrypted first decryption key and that is retained by the respective one of said plurality of clients (Ganesan, col. 6, line 49-52);

forwarding to at least a selected one of said plurality of clients said encrypted information and at least one of said entries (Ganesan, col. 10, line 46-49) in response to a request received at said file server from said selected one of said plurality of clients;

decrypting said encrypted first decryption key contained in said at least one of said entries utilizing the second decryption key corresponding to the second encryption key for the respective entry (Ganesan, col. 10, line 26-28); and



Art Unit: 2134

decrypting said encrypted information using said first decryption key to obtain said information (Ganesan, col. 10, line 45-46; col. 11, line 33).

but fail to show storing said encrypted information on said file server and storing on said file server said encrypted first decryption keys as a plurality of entries within an access control list, wherein each one of said entries is associated with one of said plurality of clients.

However Linehan teaches that accessing user is permitted to access the data file; the key server sends the key (first decryption key) corresponding to the data file to the key client of the accessing user (accessible to client); and the key client of the accessing user uses the key to decrypt the encrypted data file (Linehan, col. 5, line 13-16).

Furthermore, Linehan teaches encrypting the file encryption key (first decryption key), under the control key (group encryption key, Linehan, col. 9, line 33-34)

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Ganesan as per teaching of Linehan to provide an improved computing system having improved security in a distributed computing environment (Linehan, col. 4, line 26-28).

17. Regarding claim 15, Ganesan and Linehan disclose claim 14 above, and further discloses request includes a client identifier (first private key) associated with said selected one of said plurality of clients, said entries each include a client identifier associated with one of said plurality of clients (Ganesan, col. 10, line 66-67), and wherein forwarding includes forwarding to at least said selected one of said plurality of clients the entry including the client identifier that is associated with the client identifier contained within said request (Ganesan, col. 11, line 10-14).

Art Unit: 2134

18. Regarding claim 16, Ganesan and Linehan disclose claim 13 above, and further discloses forwarding comprises the forwarding to said selected one of said plurality of clients said encrypted information and said access control list (ticket granting ticket from ticket granting server, Ganesan, col. 4, line 40-44, col. 9, 33-34, col. 10, line 52-53).

19. Regarding claim 18, Ganesan and Linehan disclose claim 13 above, and further discloses first encryption and decryption keys are symmetric (Ganesan, col. 11, line 28-29).

20. Regarding claim 19, Ganesan and Linehan disclose claim 13 above, and further discloses first encryption key comprises one of a public key and a private key of a first public/private key pair, and the first decryption key comprises the other of said public key and said private key of said first public/private key pair (Ganesan, col. 9, line 40-41).

21. Claims 8-11 are rejected under **35 U.S.C. 103(a)** as being unpatentable over Patent No. 5,748,735, Ganesan in view of Patent No. 5,495,533, Linehan et al. in further view of "Handbook of Applied Cryptography" by Menezes et al.

22. Regarding claim 8, Ganesan and Linehan discloses claim 1 above, and further disclose entry includes said first decryption key (Ganesan, col. 10, line 39-41) wherein said data stream is encrypted with said second encryption key (Ganesan, col. 10, line 50-52); and

transmitting comprises transmitting to said client said encrypted information and said access control list key (ticket granting ticket from ticket granting server, Ganesan, col. 4, line 40-44, col. 9, 33-34, col. 10, line 52-53),

**but fail to show** that said entry includes said first decryption key combined with a check value to form a data stream.

Art Unit: 2134

Menezes teach Message Authentication Codes, MAC, (check value) where the originator of a message  $x$  (first decryption key) computes a MAC  $h_k(x)$  over the message using a secret MAC key  $k$  shared with the intended recipient and send both (effectively  $x \parallel h_k(x)$ ) (Menezes, page 364, paragraph 9.6.3, line 3-4).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Ganesan and Linehan as per teaching of Menezes to include a MAC to gain the benefit of data integrity on the stream (page 364, paragraph 9.6.3 title).

23. Regarding claim 9, Ganesan and Linehan and Menezes disclose claim 8 above and further disclose check value (secret MAC key) comprises a value known to said client (Menezes, page 364, paragraph 9.6.3, line 3).

24. Regarding claim 10, Ganesan and Linehan and Menezes disclose claim 8 above and further disclose said check value comprises an said client identifier (Menezes, page 364, paragraph 9.6.3, line 3, Ganesan, col. 9, line 40).

25. Claim 12 is rejected under **35 U.S.C. 103(a)** as being unpatentable over Patent No. 5,748,735, Ganesan in view of in view of Patent No. 5,495,533, Linehan et al in further view of "Handbook of Applied Cryptography" by Menezes in further view of Patent No. 5,787,175, Carter.

26. Regarding claim 12, Ganesan and Linehan and Menezes disclose claim 8 above and but fail to show check value comprises a group identifier that identifies a group of said client is a member.

Carter teach users who are currently members of a collaborative group can readily information (Carter, col. 6, line 12-13). Structures in the prefix portion support

Art Unit: 2134

collaborative signatures such that members of the group can digitally sign a particular version of the data (Carter, col. 6, line 16-18). An important aspect of these prefix structures is their use of public-key cryptographic (group identifier) methods (Carter, col. 6, line 25-26).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Ganesan and Linehan and Menezes as per teaching of Carter to include collaborative access control to gain the benefit to prevent unauthorized access by users whose access right have been revoked (Carter, col. 6, line 38-39).

27. Claim 20 is rejected under **35 U.S.C. 103(a)** as unpatentable over Patent No. 5,787,169, Eldridge et al in view of Patent No. 5,495,533, Linehan et al.

28. Regarding claim 20, Eldridge discloses a method for storing information securely on a file server for access by members of a group, said method comprising:

identifying the members of said group (user quorum), wherein said group has a group identifier (password key),

encrypting information with a first encryption key having an associated first decryption key (Eldridge, col. 2, line 34-37) that is usable to decrypt said encrypted information (it is obvious or inherent that the decryption key is used for decrypt encrypted information);

encrypting said first decryption key with a group encryption key having an associated group decryption key for decrypting data encrypted with said group encryption key (Eldridge, col. 2, line 43-47); and

storing said encrypted information on said file server and storing said encrypted first decryption key on said file server within an access control list (table) associated with

Art Unit: 2134

said encrypted information and containing, at least at some times, a plurality of encrypted first decryption keys (Eldridge, col. 2, line 40-48), and

but fail to show response to a request received at said file server from one of said members of said group; forwarding to said one of said members of said group said encrypted information and at least said first decryption key encrypted with said group encryption key.

However Linehan teaches that accessing user is permitted to access the data file; the key server sends the key (first decryption key) corresponding to the data file to the key client of the accessing user (accessible to client); and the key client of the accessing user uses the key to decrypt the encrypted data file (Linehan, col. 5, line 13-16).

Furthermore, Linehan teaches encrypting the file encryption key (first decryption key), under the control key (group encryption key, Linehan, col. 9, line 33-34)

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Ganesan as per teaching of Linehan to provide an improved computing system having improved security in a distributed computing environment (Linehan, col. 4, line 26-28).

29. Claims 21-30 are rejected under **35 U.S.C. 103(a)** as being unpatentable over Patent No. 5,787,169, Eldridge et al. in view of Patent No. 5,748,735, Ganesan.

30. Regarding claim 21. Eldridge discloses a method for accessing information securely stored on a file server for access by members of a group, said method comprising:

identifying the members of said group, wherein said group has a group identifier (Eldridge, col. 2, line 41-42);

Art Unit: 2134

encrypting information with a first encryption key having an associated first decryption key (Eldridge, col. 2, line 26-27, 47) that is usable to decrypt said encrypted information;

encrypting said first decryption key with a group encryption key having an associated group decryption key for decrypting data encrypted with said group encryption key (Eldridge, col. 2, line 43-47);

storing said encrypted information on said file server and storing said encrypted first decryption key on said file server within an access control list associated with said encrypted information and containing, at least at some times, a plurality of encrypted first decryption keys (Eldridge, col. 2, line 40-48);

in a first decrypting, decrypting said encrypted first decryption key with said group decryption key to obtain said first decryption key (Eldridge, col. 2, line 34-37); and

in a second decrypting, decrypting said encrypted information using said first decryption key to obtain said information (Eldridge, col. 2, line 43-47),

**but fail to show that** in response to a request received at said file server from one of said members of said group, forwarding to said one of said members of said group said encrypted information and at least said encrypted first decryption key encrypted with said group encryption key;

Ganesan teaches that a system where a symmetric crypto-key (first decryption key) is encrypted by the security server with a second private key (group encryption key) portion of the file server's crypto-key, to form a encrypted key message. The message is forwarded to the user (Ganesan, col. 6, line 17-20, 22-23).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Eldridge as per teaching of Ganesan to ensure that only the appreciate file server will have access to the symmetric crypto-key (Ganesan, col. 6, line 20-22).

31. Regarding claim 22, Eldridge and Ganesan disclose claim 21 above, and further discloses distributing said group decryption key to said members of said group and said first decrypting comprises decrypting the encrypted first decryption key by said one of said members of said group using the distributed group decryption key (Ganesan, col. 10, line 5-8).

32. Regarding claim 23, Eldridge and Ganesan disclose claim 21 and further discloses first decrypting comprises:

forwarding said encrypted first decryption key to a group server associated with said group identifier (Eldridge, col. 2, line 40-48);

decrypting said encrypted first decryption key at said group server using said group decryption key (Eldridge, col. 2, line 43-47); and

forwarding said first decryption key to said one of said group members (Ganesan, col. 10, line 50-52).

33. Regarding claim 24, Eldridge and Ganesan disclose claim 23 above, and further discloses forwarding said first decryption key to said one of said group members comprises forwarding the first decryption key to said one of said group member over a secure channel (Ganesan, col. 10, line 25-28).

34. Regarding claim 25, Eldridge and Ganesan disclose claim 24 above, and further discloses secure channel is a physically secure channel (Ganesan, col. 8, line 16-21).

Art Unit: 2134

35. Regarding claim 26, Eldridge and Ganesan disclose claim 24 above, and further discloses secure channel comprises a non-secure communications path and forwarding the first decryption key to said one of said group members over a secure channel comprises:

encrypting said first decryption key with a third encryption key having an associated third decryption key known to said one of said group members (Ganesan, col. 10, line 25-28);

forwarding to said one of said group members said encrypted first decryption key encrypted with said third encryption key (Eldridge, col. 2, line 40-48); and

decrypting by said one of said group members, said encrypted first decrypted key encrypted with said third encryption key using said third decryption key (Ganesan, col. 10, line 27).

36. Regarding claim 27, 30, Eldridge and Ganesan disclose claim 26 above, and further discloses the third encryption key comprises a public key of a member public/private key pair and wherein said third decryption key comprises the member private key of said member public/private key pair (Ganesan, col. 8, line 15-16; col. 9, line 67; col. 10, line 1-2).

37. Regarding claim 28, 29, Eldridge and Ganesan disclose claim 26 above, and further discloses third encryption and decryption keys are symmetric (Ganesan, col. 9, line 60-62).

#### ***Response to Arguments***

38. Applicant's arguments with respect to claim 1, 4-10, and 12 have been considered but are moot in view of the new ground(s) of rejection.



Art Unit: 2134

39. Applicant's arguments with respect to claim 13,15-19, and 31-37 have been considered but are moot in view of the new ground(s) of rejection.

40. Applicant's arguments with respect to claim 21-30 have been considered but are moot in view of the new ground(s) of rejection.

***Conclusion***

41. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mossadeq Zia whose telephone number is 703-305-8425. The examiner can normally be reached on Monday-Friday between 8:30am - 5:00pm.

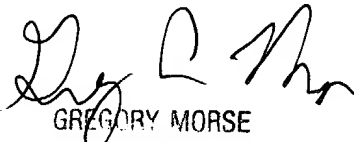
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 703-308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2134

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Mossadeq Zia  
Examiner  
Art Unit 2134

mz  
8/4/04

  
GREGORY MORSE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100